TASK ORDER (TO)

47QFCA23F0012

Enterprise Information Technology Support (EITS) Bridge Task Order 2.0

in support of:

Defense Counterintelligence and Security Agency (DCSA)

Issued to:
Deloitte Consulting LLP

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

February 8, 2023

FEDSIM Project ID 47QFCA23Z0013

C.1 BACKGROUND

On behalf of the Department of Defense (DoD), the Defense Counterintelligence and Security Agency (DCSA) plays a vital role in safeguarding our nation's information. Under the National Industrial Security Program (NISP), DCSA is the designated oversight authority on the accreditation of classified facilities, information systems, and the insider threat program. This involves security oversight of more than 10,000 companies and approximately 13,000 facilities involved in classified work throughout the DoD and 31 Federal agencies. In addition, DCSA provides counterintelligence support to cleared personnel and programs to proactively identify threats and mitigations. DCSA provides education, training, and certifications on best practices in technology and security for industry and Government personnel.

C.1.1 PURPOSE

The DCSA Office of the Chief Information Officer (OCIO) is responsible for protecting and managing the critical data stored and exchanged in execution of the DCSA mission. This data includes Governmentwide classified information for our nation's most important programs. While protecting this information, the OCIO ensures high availability of enterprise Information Technology (IT) services for DCSA mobile field support staff and global customers accessing mission applications and DCSA IT networks. The OCIO provides customer support at the Russell-Knox Building (RKB) located in Quantico, Virginia (VA) and at remote offices located within the Continental U.S. (CONUS) and Outside the Continental U.S. (OCONUS) (Hawaii). To this end, DCSA relies heavily on its contractor support under the Enterprise Information Technology Support (EITS) program.

C.1.2 AGENCY MISSION

The DCSA strengthens national security at home and abroad through its security oversight and education operations. DCSA oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under NISP by providing professional risk management services. As Functional Manager for the DoD, DCSA provides security education, training, certification, and professional development for DoD and other U.S. Government personnel, contractor employees, and representatives of foreign governments.

C.2 SCOPE

The scope of this effort is to provide enterprise IT support including program management, enterprise operational performance monitoring and reporting, call center and Service Desk (SD) support, end-user application and IT support, unified communications, server and storage Operations and Maintenance (O&M), network support, database management, asset management, application development and sustainment, Disaster Recovery (DR), and Communications Security (COMSEC). The contractor shall provide on-site support at DCSA Headquarters (HQ), secondary sites, and field offices. For remote users, the contractor shall

provide remote support at locations identified in Section F.2. Long-distance travel may be required to provide temporary support for all locations.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

a. DCSA's network infrastructure consists of non-virtual and virtual systems in multiple DCSA enclaves, data centers, regional and field offices, and in the Amazon Web Service (AWS) Govcloud environments.

b. DCSA's enclaves include: Pre-Production, Production, Non-classified Internet Protocol Router Network (NIPRNet), Secret Internet protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communication System (JWICS), and DCSA's multiple cloud instances.

c. DCSA's datacenters supported by this TO are located in RKB Quantico, VA; Fort (Ft.) Meade, MD; Boyers, PA; Seaside, California (CA); Farmers Branch, Texas (TX); and Phoenix, Arizona (AZ).

d. For Web Content, DCSA currently uses Defense Media Activity Platform; however, the contractor may be required to support the implementation of other new technology solutions/platforms within DCSA's current and future environments.

e. The following technologies are required to support DCSA's IT environment for this work: Adobe Creative Suite, Adobe Creative Cloud – Dreamweaver, and other Adobe specialized tools, Microsoft (MS) Office Suite, Splunk, Oracle, SQL Server, Solar Winds, ServiceNow, MySQL, Visual Studio, Windows Operating System (OS), and any other web solution technology approved by DCSA. Additionally, DCSA is migrating to DoD Office 365 environment as part of the DISA tenant.

f. For SharePoint, DCSA currently uses the DoD/Defense Information Systems Agency (DISA), Enterprise Portal Services; however, the contractor may be required to support the implementation of other new technology solutions/platforms within DCSA's current and future environments.

g. The contractor shall be responsible for managing Data Center East (DCE) networks (comprised of NIPR, SIPR, and JWICS) and Data Center West (DCW) (NIPR only), and all associated infrastructure. DCE is also comprised of North Atlantic Treaty Organization (NATO), Insider Threat internal, and a Federal Bureau of Investigations (FBI) networks, for which the contractor shall only be responsible for managing network access connections.

C.4 OBJECTIVE

The objective of the EITS effort is to deliver a highly secured and adaptable IT infrastructure, world-class customer support, and cutting-edge technologies that support the operations and advancement of the DCSA mission. Inherent to this objective is the task of creating a more collaborative, integrated, transparent, predictable, and measurable organization. Additionally, the EITS effort will lead the IT enterprise as a change agent for adopting best practices in governance and information sharing. The end result of these efforts will enable DCSA to foresee the needs of its IT customers, make informed enterprise IT decisions and investments, and rapidly respond to mission priorities.

C.5 TASKS

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 SUBTASK 1.1 – ACCOUNTING FOR SERVICE CONTRACT REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DCSA. The contractor shall completely fill in all required data fields using the following web address: http://www.sam.gov.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.sam.gov.

C.5.1.2 SUBTASK 1.2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section J, Attachment E) (Section F, Deliverable 1.1). The MSR shall include the following:

a. Activities during the reporting period, by task (include ongoing activities, new activities, activities completed, and progress to date on all above-mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
g. Cost incurred by CLIN.
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.

C.5.1.3 SUBTASK 1.3 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly Technical Status Meeting on-site at DSCA HQ with the DSCA Technical Point of Contact (TPOC), FEDSIM COR, and other Government stakeholders (Section F, Deliverable 1.2). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including

attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR within five workdays following the meeting (Section F, Deliverable 1.3).

Additionally, the contractor shall convene an After-Action Meeting (Section F, Deliverable 1.4) following major outages and issues (i.e., Priority 1) that occur during performance of the contract. The meeting shall include the contractor's Subject Matter Experts (SMEs) and appropriate Government personnel. The purpose of the meeting is to discuss the information provided in the After-Action Report (AAR) (Section F, Deliverable 1.4) and lessons learned.

C.5.1.4 SUBTASK 1.4 – PREPARE AND UPDATE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP and shall provide it to the Government (Section F, Deliverable 1.6).

The PMP shall:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, format, and other rules of engagement between the contractor and the DCSA divisions and FEDSIM
g. Include the contractor's Quality Management Plan (QMP) (Section F, Deliverable 1.10).

The PMP is an evolutionary document that shall be updated as necessary. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.5 SUBTASK 1.5 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 1.9). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, Trip Reports shall be prepared with the information provided in Section J, Attachment F.

C.5.1.6 SUBTASK 1.6 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a QMP and maintain and update it as changes in the program processes are identified (Section F, Deliverable 1.10). The contractor's QMP shall describe the application of the appropriate methodology (e.g., quality control and/or quality assurance) for accomplishing TO performance

expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

C.5.1.7 SUBTASK 1.7 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan within four weeks of PS (Section F, Deliverable 1.11). The contractor shall review and update the Transition-Out Plan in accordance with the specifications in Sections E and F.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Program management processes.
b. POCs.
c. Location of technical and program management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Schedules and milestones.
h. Actions required of the Government.
i. Physical transfer of any Government-Furnished Property (GFP)

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

C.5.2 TASK 2 – CUSTOMER SUPPORT (CS)

The first POC and customer service interface for all service requests related to DCSA's IT environment and mission applications is CS. To provide guidance, support, and resolve issues in a timely manner, CS communicates through a variety of continually changing customer channels (currently walk-in, telephone, email, and web inquiries). CS operates a call center for mission applications, first call resolution for IT service requests, and dispatch-ready technicians to assist HQ and DCSA field support staff. CS is responsible for the coordination, resolution, and closure of all service requests beyond first call resolution.

In execution of Task 2 requirements, the contractor shall implement a CS program using industry best practices. The contractor shall identify business practices, technologies, and automation in the services it provides that achieve efficiencies in task performance and improve customer experience. The contractor shall implement information sharing and knowledge management capabilities, continuous process improvement, and performance tracking and monitoring capabilities. The contractor shall ensure customer satisfaction benchmarks and current metrics are tracked and made transparent via a shared portal (i.e., Service Now). The contractor shall maintain and provide awareness and transparency on Service Level Agreements (SLAs) and performance measurements within this task. The contractor shall develop, update, and maintain a rigorous Lifecycle Management Plan (LCMP) for all task equipment, software, and hardware in

coordination with Asset Management (C.4.5). The contractor shall provide weekly, monthly, and ad-hoc reports as required (Section F, Deliverables 2.1, 2.2, and 2.4).

C.5.2.1 SUBTASK 2.1 – KNOWLEDGE CENTER (KC)

The DCSA KC is the single POC for customer service support on DCSA's portfolio of mission applications. This portfolio currently includes the Industrial Security Facilities Database (ISFD); NISP Central Access Information Security System (NCAISS); Security Training, Education, and Professionalization Portal (STEPP); Office of the Designated Approving Authority (ODAA) Business Management System (OBMS); and National Industrial Security System (NISS). The portfolio of applications is subject to change over the course of the contract. KC is responsible for responding to customer service requests, providing account management, opening/closing service request tickets, performing first call resolution, and coordinating and escalating issues when necessary.

The contractor shall:

a. Provide O&M support of the KC.
b. Update and maintain the Standard Operating Procedures (SOPs) for the KC (Section F, Deliverable 2.5).
c. Provide user account administration and creation, assist with user registration, and respond to user account requests.
d. Respond, troubleshoot, and resolve technical user account errors/issues.
e. Document, track, and analyze customer service requests.
f. Document and track call metrics, service request/resolutions, and trend analysis to implement measures that prevent recurring problems and improve customer experience (Section F, Deliverables 2.1 and 2.2).
g. Recommend and implement technical and/or management capabilities that improve the KC's operational effectiveness.
h. Provide user training and internal knowledge transfer as required.

C.5.2.2 SUBTASK 2.2 – IT SERVICE DESK (SD)

The DCSA IT SD is the single POC for DCSA enterprise IT-related support. The SD currently operates a separate call center from the KC leveraging the same call manager. The SD receives service requests through all accessible communication channels and utilizes an enterprise ticket management system (Remedy) to track and monitor service requests. The SD is responsible for responding to, prioritizing, and coordinating resolution of service requests residing on DCSA networks (Non-classified Internet Protocol Router (NIPR)/ Secret Internet Protocol Router (SIPR)/ Joint Worldwide Intelligence Communication System (JWICS)/ Battlefield Information Collection and Exploitation System (BICES)/Insider Threat-Internal). The SD provides remote support as well as on-site support for customers at the RKB, the Center for Development of Security Excellence (CDSE), regional and local field offices, other remote locations, and Very Important Persons (VIPs) as necessary. The SD includes a geographically dispersed team of technicians located across DCSA locations identified in Section F.2. On-site (permanent) support is required in accordance with the locations identified in Section F.2. Over the life of the contract, DCSA regional and field offices will be transitioning to a JWICS environment.

The contractor shall:

a. Provide O&M support of the SD.
b. Update and maintain the SOPs for the SD (Section F, Deliverable 2.5).
c. Provide a first POC helpdesk for all enterprise IT service requests.
d. Provide timely acknowledgement of service requests, problem identification, root cause analysis, escalation, resolution, and closure for all service requests. Response to service requests shall be based on the DCSA prioritization level and SLAs identified by the Government.
e. Provide a mechanism that offers status on service requests for users (e.g., automated self-accessible portal or through direct follow-up communication).
f. Provide a user self-help capability, such as tier 0, and continually enhance self-service capabilities to resolve issues for users to reduce service requests.
g. Provide end-user account administration services (add/change/remove) and password resets.
h. Provide deskside support to resolve customer service requests.
i. Coordinate escalation of service requests to regional and field office technicians and other third parties, such as hardware and software suppliers, Original Equipment Manufacturers (OEMs), third-party DCSA contractors, and other DCSA internal technical support.
j. Document and track call metrics, service request/resolutions, and trend analysis (Section F, Deliverables 2.1 and 2.2) to implement measures that prevent recurring problems and improve customer experience. Trend analysis and reporting shall be customized based on the request of the Government (may request details on the type of technical issue, location, tier, etc.).
k. Provide situational awareness throughout DCSA on IT-related issues impacting the enterprise.
l. Recommend and implement technical and/or management capabilities that improve the SD's operational effectiveness.
m. Provide the DCSA TPOC with a Weekly Status Report (Section F, Deliverable 2.1) on all call and service metrics.
n. Provide customer service satisfaction measurements (e.g., surveys) (Section F, Deliverable 2.2).
o. Provide training and knowledge transfer as required.
p. Maintain call-in responsibility in the event of RKB closure.

C.5.2.3 DESKTOP ENGINEERING/AUTOMATION

Desktop Engineering/Automation supports deployment, maintenance, and troubleshooting of various technologies across all enclaves (NIPR/SIPR/JWICS). The desktop support team is an extension of the customer support team and is also responsible for timely resolution of service requests, incidents, and issues. Service requests are managed, tracked, and updated through the enterprise ticket management system. All Desktop Engineering/Automation services must conform to the latest DoD information security policies and timelines.

The contractor shall:

a. Update and maintain the SOPs to support desktop engineering/automation (Section F, Deliverable 2.5).
b. Provide day-to-day operations for desktop engineering/automation tasks.
c. Provide timely service and resolution of service requests and incidents in accordance with the SLAs.
d. Build, image, update, maintain, and secure DCSA enterprise endpoints.
e. Ensure all baseline configurations across endpoints are done securely with Security Technical Implementation Guides (STIG) compliance in accordance with DoD mandates.
f. Ensure appropriate testing of desktop packages is completed prior to deployment.
g. Troubleshoot and make recommendations to the Government for remediation of security or functionality issues in the desktop image.
h. Perform patches in accordance with DoD authorized timelines.
i. Coordinate resolution of desktop incidents and issues with the appropriate DCSA team (e.g., Data Center Operations (DCO)).
j. Ensure all service requests and issues are tracked and documented.
k. Recommend and implement technology, knowledge management, and processes that improve the effectiveness of desktop engineering/automation.
l. Identify problematic trends and patterns and recommend solutions.
m. Document desktop system configuration, network configuration, and inventory of software to be supported.
n. Provide training and knowledge transfer as required.

C.5.2.4 SUBTASK 2.4 – COMMUNICATIONS SECURITY (COMSEC)

COMSEC is the system of security measures used to protect classified information or material utilizing cryptographic keying material and equipment. COMSEC measures are taken to deny unauthorized personnel information derived from telecommunications of the U.S. Government concerning national security and to ensure the authenticity of such telecommunications. COMSEC includes cryptography, transmission security, and physical security of COMSEC material and information. DCSA utilizes the services of the National Security Agency's (NSA) COMSEC Office of Record. The contractor shall assist the DCSA COMSEC Manager in performing the functions and responsibilities of securing equipment, materials, and information. All services shall be performed in accordance with the DoD and Intelligence Community (IC) COMSEC policies and procedures.

The contractor shall:

a. Update and maintain the SOPs for COMSEC activities (Section F, Deliverable 2.5).
b. Serve as a custodian for DCSA COMSEC account(s) and perform COMSEC custodian duties including, but not limited to, receipt, custody, issuance, safeguarding, accounting for, and, when necessary, destruction of COMSEC material for offices and/or field operations under their areas of responsibility.
c. Maintain up-to-date records of COMSEC inventory and submit required accounting reports in accordance with policies and procedures (Section F, Deliverable 2.3).
d. Administer initial briefings and debriefings to individual users and maintain copies of all.

e. Ensure all hired personnel supporting COMSEC requirements undergo required NSA COMSEC training within the required performance timelines.
f. Conduct programming and local distribution of COMSEC devices including, but not limited to, Secure Telephone Equipment (STE), Sectera vIPer Universal Secure phone, and network encryptor solutions (e.g., Tactical Local Area Network Encryptions (TACLANEs)).
g. Provide order, receipt, loading, and management of COMSEC keying material using devices such as the Key Management Infrastructure (KMI), Simple Key Loader (SKL), and other devices as necessary.
h. Ensure all COMSEC Element accounts are in compliance with NSA policies.
i. Provide technical and administrative support to COMSEC equipment holders, documenting within DCSA's Service Support system.
j. Evaluate new COMSEC equipment and fax machines for use by DCSA.
k. Maintain a stock of COMSEC equipment to provide immediate replacement of operational equipment for use in establishing emergency circuits and to replace equipment in need of repair.
l. Provide technical support to DCSA to facilitate interoperability of purchases of COMSEC equipment.
m. Re-key all circuits as required.
n. Assist in properly storing, managing, and maintaining accountability within KMI on all COMSEC material and assets.
o. Maintain COMSEC access list for DCSA COMSEC Controlled/Closed Area Designations.
p. Ensure prompt and accurate preparation, signature, and submission of account correspondence, message, and accounting reports.
q. Conduct periodic spot checks to ensure clearances listed are actually held and valid.
r. Provide COMSEC training and knowledge transfer as required.

C.5.2.5 SUBTASK 2.5 – UNIFIED COMMUNICATIONS (UC)

UC is comprised of Video Conferencing (VTC), Audio/Visual (A/V), collaboration services, voice services, and mobile solutions. UC endpoints reside on unclassified and classified (NIPR/SIPR/JWICS) networks.

The contractor shall:

a. Update and maintain the SOPs that support unified communications (Section F, Deliverable 2.5).
b. Provide O&M support for all UC capabilities including, but not limited to, VTC, Voice, A/V, instant messaging, and mobile communications.
c. Provide VTC provisioning, setup, configuration, call scheduling, and problem management.
d. Design and engineer UC solutions.
e. Recommend improvements to the existing service catalog of offerings and implement new capabilities.

f. Provide conference room A/V and VTC support including setting up, designing, configuring, troubleshooting, operating, and sustaining UC devices.
g. Provide support for mobile telephone service deployments, account setup with provider, troubleshooting, configuration, and migration to provider services.
h. Provide coordination and resolution with the DoD Mobility Classified and Unclassified Capability (DMCC/UC) in support of mobile device management services.
i. Provide mobile device end-user support and incident resolution including, but not limited to, device setup and configuration, problem resolution, hotspot management, application support, and email configuration.
j. Troubleshoot and resolve DoD enterprise email service requests in coordination with Defense Information Systems Agency (DISA).
k. Provide inventory management, specifications, and compliance for all assigned devices in coordination with asset management.
l. Provide wireless billing management including, but not limited to, invoice reconciliation, usage and billing analysis, and recommending efficiencies in wireless usage.
m. Conduct end-user training on UC equipment capabilities.
n. Provide A/V setup, configuration, troubleshooting, and maintenance.
o. Provide Voice over Internet Protocol (VoIP) desk phone support including deployments, troubleshooting, configuration, problem management, training, and maintenance.
p. Provide weekly, monthly, and ad-hoc reports regarding UC incident reporting (by category and region) and resolution (Section F, Deliverables 2.1, 2.2, and 2.4).

C.5.2.6 SUBTASK 2.6 – CDSE CLASSROOM AND END-USER SUPPORT

Customer support is provided on-site at CDSE for faculty, staff, students, and instructors. CDSE support includes the classroom setup, IT equipment and network configuration, desktop support, teleconference, A/V, communications, and room tear-down. The scope of CDSE support performed under this contract is limited to IT support and does not include CDSE formal training offerings.

The contractor shall:

a. Update and maintain Classroom Support SOPs (Section F, Deliverable 2.5).
b. Image/re-image laptops with the correct version of the approved image in the current Configuration Management Database (CMDB) and in accordance with current cybersecurity policy for student laptop use.
c. Maintain configuration documentation as needed (e.g., special instructions for software installation and configuration, network configuration, Windows Server Update Service (WSUS) management, and other classroom-specific IT support requirements).
d. Configure in-classroom equipment, printers, sound, and other systems in support of instructors.
e. Setup and remove audio-phone devices to be used in classroom spaces (e.g., desktop speaker phones).
f. Ensure the CDSE student environment complies with current DCSA Information Assurance (IA) policy and guidance, such as updating accreditation documentation, scanning, remediation, and other support as required.

g. Customize the images as needed to meet instructor requirements.
h. Recommend and implement improvements and automations to the student environment and services.
i. Assist with the duplication of class materials for distribution to the students prior to the instructor-led course (e.g., CD or DVD duplication). Duplications will be made at least three business days prior to requiring the materials for distribution. All materials will be requested by the customer through the SD ticketing system.
j. Assist with properly connecting approved systems for projector display, audio, or network in conference or meeting rooms (only DCSA Government-Furnished Equipment (GFE) may connect to the NIPR Network (NIPRNet)).
k. Provide user training and knowledge transfer as required.
l. Conduct inventory of all CDSE property and equipment and follow accountability procedures in accordance with the SOP.
m. Document, track, and conduct trend analysis on CDSE service requests (Section F, Deliverables 2.1 and 2.2).

C.5.3 TASK 3 – DATA CENTER OPERATIONS (DCO)

DCO supports HQ Data Center East (DCE), the DR Boyers, a small server and storage environment in Linthicum, MD. The contractor shall be responsible for managing DCE networks (comprised of NIPR, SIPR, and JWICS), Boyers (NIPR only), and all associated infrastructure. DCE is also comprised of North Atlantic Treaty Organization (NATO), Insider Threat internal, and a Federal Bureau of Investigations (FBI) network for which the contractor shall only be responsible for managing network access connections. The contractor shall be responsible for managing the Storage Area Network (SAN) and server environment located in Linthicum, MD. The contractor shall support the transition of all Virtual desktop infrastructure (VDI) users. Additionally, DCSA anticipates deploying JWICS to field offices over the course of the contract. The contractor shall support the transition of field offices to JWICS.

In execution of Task 3 requirements, the contractor shall provide a flexible enterprise IT environment that can meet changing strategic goals and priorities as well as demands for capacity and new capabilities that support the DCSA mission. The contractor shall provide the expertise, best practices, and agility to meet the constant changes and evolution of the enterprise IT environment. The contractor shall maintain working partnerships at all levels of the DCSA organization (strategic, tactical, and operational) in order to cohesively design, implement, and maintain networks, systems, applications, and technology within the enterprise. The contractor shall work with all parts of the organization including, but not limited to, CS, Configuration, Change and Release Management (CCRM), and OCIO (including other third-party contractors) to integrate and improve. The contractor shall coordinate with third-party vendors and contractors to ensure technology roadmaps are part of the overall DCO LCMP. The contractor shall assist with developing the enterprise architecture plans and technology roadmaps and continually evaluate business cases for new technologies in the enterprise. The contractor shall maintain awareness and transparency on SLAs and performance measurements within the task. The contractor shall develop, update, and maintain a rigorous LCMP for all task equipment, software, and hardware in coordination with Asset Management (C.4.5). The contractor shall provide weekly, monthly, and ad-hoc reports (Section F, Deliverables 1.1, 3.14, and 3.15) as required.

C.5.3.1 SUBTASK 3.1 – NETWORK SUPPORT

The DCSA current network environment consists of NIPR, SIPR, JWICS, NATO, Insider Threat internal, and FBI networks. Network support includes engineering, O&M, administration, and security for all enclaves. The contractor shall conduct planning, design, configuration, troubleshooting, implementation, security, operations, and management for all DCSA networks. All network services shall be performed in accordance with the latest DCSA and DoD policies and procedures. Network support may be required on-site at field offices identified in Section F.2.

C.5.3.1.1 ENGINEERING, OPERATIONS, AND ADMINISTRATION

The contractor shall:

a. Update and maintain the SOPs for network engineering, operations, and administration activities for all enclaves (Section F, Deliverable 2.5).
b. Develop, update, and maintain plans, designs, and architecture documentation (Section F, Deliverable 3.1) for all network enclaves in support of this task.
c. Recommend and implement changes, enhancements, and improvements to existing network equipment to optimize performance and security.
d. Perform day-to-day network operations and administration activities.
e. Monitor and manage bandwidth requirements; conduct capacity planning to ensure appropriate bandwidth management; and ensure network provisioned gear is documented.
f. Operate and maintain network test and development environments.
g. Maintain physical devices, firmware updates, Operating System (OS) changes, and security releases.
h. Perform integration and testing on all equipment, systems, software, hardware, configurations, appliances, and other items in coordination with the appropriate parties.
i. Ensure network infrastructure is secured and operational before deploying.
j. Provide tuning to maintain optimum performance across the network.
k. Provide installation, upgrades, configuration, troubleshooting, maintenance, and optimization on Wide Area Network (WAN)/Local Area Network (LAN) routers, switches, firewalls, circuits, and other necessary equipment.
l. Provide load balancing (F5 BigIP) and traffic load balancing support for all enclaves.
m. Identify and resolve network problems in coordination with the SD as required.
n. Coordinate with third-party carriers, vendors, and technology providers to troubleshoot and perform operations activities.
o. Serve as a liaison between outside agencies, third-party providers, or other vendors to perform network activities as required.
p. Managing router/switch configurations, firewalls, Internet Protocol (IP) addresses and related services, such as Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP).
q. Maintain all DCSA internet, NIPR, SIPR, and JWICS access points.
r. Ensure configuration documentation is accurate and completed for all changes. Coordinate with Configuration Management (CM) to ensure any new or updated records for configuration items are recorded in the CM system.

s. Manage site-to-site Virtual Private Network (VPN) connectivity including, but not limited to, design, installation, configuration, documentation, and problem/resolution (Section F, Deliverable 3.2).
t. Develop, update, and maintain existing and future CM and change control documentation including, but not limited to, network and system specifications, topologies, diagrams, and policies (Section F, Deliverable 3.3).
u. Consult with DCSA IT groups to develop and implement a standard architecture for access control points, such as firewalls and Access Control Lists (ACLs).
v. Track endpoint devices and configure changes.
w. Design, implement, and configure security and firewall solutions in coordination with Computer Network Defense (CND).
x. Provide logical network data flow diagrams for each application assessed (Section F, Deliverable 3.4).
y. Conduct data trend analysis on network management activities (e.g., using monitoring tools) and provide reports to the DCSA TPOC (Section F, Deliverable 1.1).
z. Provide training and knowledge transfer as required.
aa. Provide engineering capability assessments to ensure the network capability is meeting current agency demands; plan, design, and implement capabilities when the demand is no longer being met.
bb. Update the DCSA Run Book as needed (Section F, Deliverable 3.5).
cc. Provide IA system validation and assessments.
dd. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).

C.5.3.1.2 NETWORK SECURITY

In support of this Network Security task, the contractor shall:

a. Update and maintain the SOPs to support network security activities (Section F, Deliverable 2.5).
b. Conduct vulnerability assessment audits, develop Plan of Action and Milestones (POA&Ms) to be submitted to the appropriate DCSA management, and execute patching and updates for all systems in order to maintain current DoD compliance.
c. Install, configure, and test patches and changes required by Vulnerability Management System issuances (i.e., Information Assurance Vulnerability Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVBs), Information Assurance Vulnerability Management (IAVM), STIGs) in accordance with the suspense date articulated by the Government authority. All patches shall be tested in pre-production and scheduled with the Government prior to deployment.
d. Maintain the network Certification and Accreditation (C&A) documentation (DoD IA C&A Process/Risk Management Framework (RMF)) for all specialized network systems, software, and hardware used on DCSA networks in accordance with applicable DoD policies.
e. Develop reports on security vulnerability trends and analysis (Section F, Deliverable 1.1).
f. Provide training and knowledge transfer in accordance with the performance metrics.

g. Review and provide recommendations to improve current processes and procedures.
h. Provide ad-hoc reports as required.
i. Provide IA system validation and assessments.
j. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (i.e., eMASS).

C.5.3.2 SUBTASK 3.2 – SERVER OPERATIONS AND ADMINISTRATION

DCSA server infrastructure consists of virtual and non-virtual servers in cloud development environments, pre-production and testing, production, and fail-over enclaves. The contractor shall be responsible for infrastructure asset lifecycle maintenance and ensuring the infrastructure is maintained and secured in all enclaves. The contractor shall provide reliable, high availability services and optimize server infrastructure to achieve high performance and cost-efficiencies for virtual and non-virtual systems. The contractor shall improve scalability, surge, and automation capabilities to support the potential expansion of capabilities and storage throughout the life of the contract. The contractor shall maintain all configurations in accordance with DoD policies and procedures.

The contractor shall:

a. Update and maintain the SOPs to support server operations and administration (Section F, Deliverable 2.5).
b. Develop, update, and maintain existing and future server and system diagrams (Section F, Deliverable 3.6).
c. Provide maintenance to all server infrastructure components (i.e., OS down to the firmware) and maintain a secure server configuration.
d. Monitor enterprise operations (System Center Operations Manager (SCOM)), system configurations, and traffic, and provide optimization in health and performance.
e. Provide domain administration services including, but not limited to, system and data access, share management, elevated privilege accounts report, access/activity log searches, account creation, and user access rights.
f. Test and deploy patches and updates.
g. Provide capacity management for enterprise computing resources including proactively recommending and planning upgrades and replacements.
h. Provide controls, access, and management enterprise input and output resources (e.g., scanners, printers, and files).
i. Provide Add/Move/Change for printers and other devices.
j. Provide encrypted system backups and off-site storage in accordance with DCSA policies and procedures.
k. Provide system and data restoration in accordance with EITS SLAs.
l. Provide archiving of mailbox (legacy email), file data, and user information.
m. Provide ad-hoc reports as required.
n. Ensure the VDI enclave is maintained to meet agency demands and performance.
o. Provide training and knowledge transfer.

p. Provide engineering capability assessments to ensure server administration capabilities are meeting current agency capacity demands; plan, design, and implement capabilities when the capacity demand is no longer being met.
q. Update the DCSA Run Book as needed (Section F, Deliverable 3.5).
r. Provide IA system validation and assessments.
s. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).

C.4.3.3 SUBTASK 3.3 – STORAGE OPERATIONS AND ADMINISTRATION

The contractor shall:

a. Update and maintain the SOPs to support storage operations and administration (Section F, Deliverable 2.5).
b. Perform O&M for the distributed storage enclaves.
c. Implement and maintain storage and backup solutions.
d. Update and maintain existing and new storage architectures (including SAN interconnections) for DCSA enclaves (Section F, Deliverable 3.7).
e. Monitor storage availability, capacity, and performance and provide reports and trend analysis for capacity planning for all enclaves (Section F, Deliverable 3.8).
f. Perform enterprise storage data analysis (search and purge) to reduce capacity.
g. Provision, de-provision), install, and configure storage solutions in accordance with STIG compliance.
h. Coordinate and conduct incident resolution on storage-related issues.
i. Monitor and manage physical drives (e.g., failures and replacements).
j. Perform Network Attached Storage (NAS)/Fabric Attached Storage (FAS) management for storage.
k. Provide training and knowledge transfer in accordance with the performance metrics.
l. Provide engineering capability assessments to ensure storage capabilities are meeting current agency capacity demands; plan, design, and implement capabilities when the capacity demand is no longer being met.
m. Update the DCSA Run Book as needed (Section F, Deliverable 3.5).
n. Provide IA system validation and assessments.
o. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).
p. Coordinate with third-party vendors and technology providers to troubleshoot and perform operational activities.

C.5.3.4 SUBTASK 3.4 – DATABASE MANAGEMENT

The contractor shall provide database management services for databases residing on DCSA networks. The contractor shall provide database administration support, including modifications to any system or production application database and pre-production database. The contractor shall perform schema changes and conversion of the production database during application upgrades and new version releases.

The contractor shall:

a. Update and maintain the SOPs to support database management (Section F, Deliverable 2.5).
b. Provide lifecycle database management services including, but not limited to, design, development, provisioning, creation, modifying and managing data and schema, cloning and backup, troubleshooting, account management, and decommissioning.
c. Maintain databases, clusters and replications for pre-production, productions, and backup; ensure current application upgrades and releases are timely.
d. Provide database metrics, such as growth and usage of capabilities, and recommend new capabilities as needed.
e. Perform database optimization.
f. Coordinate with third-party vendors on database issues and resolution.
g. Conduct daily database operations checks and status report (Section F, Deliverable 3.9).
h. Provide training and knowledge transfer as required.
i. Provide scripting to support database content and reporting.
j. Develop database dictionaries for all databases in support of this task.
k. Update the DCSA Run Book as needed (Section F, Deliverable 3.5).
l. Provide IA system validation and assessments.
m. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).

C.4.3.5 SUBTASK 3.5 – DISASTER RECOVERY (DR)

The DR site (located in Boyers, Pennsylvania (PA)) is considered a cold/warm site with no active users unless a failover is initiated. Applications are on a “cold” standby and databases are considered “warm” due to real-time replication.

In support of DR events, the contractor shall fully implement its DR Plan (Section F, Deliverable 3.10) immediately upon Government or Helpdesk notification or through self-analysis that production services have failed. This includes restoration of all DCSA production systems and data. The contractor shall update and maintain the IT system DR Plan and be available to perform testing and validation of its plan and procedures. The contractor shall produce and maintain an IT Operations Run Book (also known as the SOP) that provides detailed instructions on the IT system DR process. The Operations Run Book shall be updated as required to stay current. The DR plan shall be maintained and executed in accordance with DoD policies and mandates.

The contractor shall:

a. Update and maintain DR Plan that supports the DCSA strategy, requirements, scenarios, and recovery time/position objectives and resiliency/redundancy requirements for IT infrastructure and systems (Section F, Deliverable 3.10).
b. Conduct training and establish scheduled DR tests; track and report DR test results and lessons learned; and incorporate lessons learned into the DR Plan (Section F, Deliverable 3.11).

c. Recommend and approve data (e.g., File System, Database, and Flat Files) replication, backup, and retention requirements.
d. Provide ad-hoc reporting as required.
e. Perform failover tests and provide feedback to the IA Branch.
f. Monitor and manage Hard Disk Drives (HDDs), tape library, and library physical drives (i.e., failures and replacements).
g. Support relocation planning and transition DR infrastructure.
h. Update and maintain existing and new DR architectures for all DCSA enclaves (Section F, Deliverable 3.12).
i. Monitor DR availability, capacity, and performance and provide reports and trend analysis for capacity planning (Section F, Deliverable 3.13).
j. Perform enterprise DR data analysis (search and purge) to reduce capacity.
k. Provision, de-provision, install, and configure DR solutions in accordance with STIG compliance.
l. Provide engineering capability assessments to ensure DR capabilities are meeting current agency capacity demands; plan, design, and implement capabilities when the capacity demand is no longer being met.
m. Update the DCSA Run Book as needed (Section F, Deliverable 3.5).
n. Provide IA system validation and assessments.
o. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).

C.5.4 TASK 4 – APPLICATION SUPPORT

The contractor shall develop and implement a mature lifecycle process for conducting application development and sustainment of DCSA applications. The contractor shall establish collaborative, working relationships across DCSA to ensure applications being developed are successfully transitioned and maintained. The contractor shall develop, update, and maintain a rigorous LCMP for all task equipment, software, and hardware in coordination with Asset Management (C.4.5). The contractor shall provide weekly, monthly, and ad-hoc reports (Section F, Deliverables 1.1, 4.1, and 4.17) as required.

C.5.4.1 SUBTASK 4.1 – APPLICATION DEVELOPMENT

The contractor will be required to provide application development support under this contract. In such cases, the application sustainment team (C.4.4.2) shall be responsible for conducting a quantitative code assessment to determine the scope of development support required. The Government will provide advanced notice and approval to the contractor to begin planning software maintenance/development efforts. The contractor shall provide a Project Management Plan (Section F, Deliverable 4.2) at the beginning of the project. Application maintenance/development efforts may include, but are not limited to, custom, Commercial off-the-Shelf (COTS), Government off-the- Shelf (GOTS), open source, and web-based applications.

The requirements for development under this task are limited to applications that have already been or are planning to be deployed into the DCSA production baseline. The following provides the anticipated level of effort for changes required for deployments.

Medium-Sized Deployments: DCSA anticipates executing a total of two medium-sized releases or deployments each year. These medium-sized deployments shall consist of a roughly six-month project lifecycle consisting of planning through execution and closeout. A medium-sized release is defined as more than 10 percent and up to 25 percent of application code changes, through the deployment of patches, software/hardware component refreshes, or bug fixes.

Large-Sized Deployments: DCSA anticipates executing one large release or deployment each year. This large deployment will consist of roughly a 12-month duration to execute a full project lifecycle consisting of planning through execution and closeout. A large release is defined as more than 25 percent and up to 50 percent of application code changes.

C.5.4.1.1 PLANNING, REQUIREMENTS DEVELOPMENT, AND DESIGN

In support of planning, the contractor shall review the quantitative code assessment and the Government's request for application development support. The contractor may request additional information in order to develop a project plan. Based on the project request, the contractor shall develop a comprehensive Development PMP that identifies preliminary scope, quality, schedule, resources, risks, costs, and communications (Section F, Deliverable 4.2).

Upon Government approval of the Development PMP, the contractor shall begin performing full Software Development Lifecycle (SDLC) activities. The contractor shall develop concept documentation and requirements and design documentation. The contractor shall work with DCSA stakeholders, O&M staff, and users to gather requirements that address user functionality, DCSA architecture guidelines, and security requirements. Prior to development, the contractor shall provide technical design documentation (Section F, Deliverable 4.3) to be reviewed/approved by the Government. The technical design shall include formal requirements documentation and mock-ups of proposed changes. The mock-ups may include modified screen captures from an actual application under development. The contractor shall inform the Government of any issues that arise or changes that may impact the scope, schedule, or costs to the project.

The contractor shall provide weekly status reports on the progress of projects (Section F, Deliverable 4.1).

C.5.4.1.2 DEVELOPMENT

Upon Government approval of the technical design documentation, the contractor shall perform Agile-based or iterative development activities that allow for frequent delivery of application changes. The contractor shall use industry best practices and methodologies when performing development. The contractor shall use baselined cost and schedule for assessment of planned versus actual performance. The contractor shall inform the Government of risks, impacts, and potential changes to the project scope, schedule, costs, and product quality.

The contractor shall:

a. Deliver an Integrated Master Schedule detailing planned versus actual activities (project scope, schedule, costs, and product quality) (Section F, Deliverable 4.4).
b. Provide Risk Management with establishment and maintenance of a Risk Register including identified risks, qualitative analysis, triggers, and responses (Section F, Deliverable 4.5).
c. Provide meeting agendas, meeting minutes, action logs, and risk registers in support of weekly status meetings (Section F, Deliverable 4.1).

d. Escalate issues that arise during development to the Government with an Issue Impact Analysis Report (Section F, Deliverable 4.6).
e. Develop a Resource Breakdown Structure (RBS) that provides full visibility on resource allocation and schedules (Section F, Deliverable 4.7).
f. Provide system accreditation support and documentation (Section F, Deliverable 4.8).
g. Provide documentation on development activities to address knowledge transfer with the O&M team.

In addition, the contractor shall provide the following lifecycle development deliverables (Section F, Deliverable 4.9):

a. Software code/software code integration.
b. Release summary report.
c. System architecture/design docs with process flow diagrams.
d. Technical requirements documentation.
e. Requirements traceability matrix.
f. Network typology.
g. Installation/user guide.
h. RMF compliance documentation.
i. Deployment plan.
j. Data dictionary with meta-data mapping (Schema).

C.5.4.1.3 PRE/POST TESTING REVIEWS

Prior to submitting application code changes or software upgrades for production usage, the contractor shall perform preliminary internal testing to identify and address test findings. The contractor shall utilize industry best practices and methodologies in testing. Testing results shall be documented in a Test Report that identifies resolved and outstanding contractor test findings (Section F, Deliverable 4.10). The contractor's Test Report shall serve as an input into the formal Independent Verification and Validation (IV&V) testing performed by a third-party contractor. All application code changes or software upgrades will undergo formal DCSA IV&V testing.

A Test Readiness Review (TRR) is scheduled prior to IV&V. The TRR serves as a validation point for stakeholder requirements and presents mock-ups in comparison to the delivered changes. It ensures that the system is ready for testing, by having been delivered, installed, and operating with functioning testing accounts. The Test Report is reviewed prior to formal testing.

Post Test Acceptance Review (PTAR) is conducted at the conclusion of testing. DCSA Operational Test and Evaluation (OT&E) test findings shall be reviewed, and recommendation shall be provided for production deployment or referred back to the contractor for rework. Unless granted an exception through waiver, findings assigned a Critical or High severity will be returned to the contractor for rework.

At least one member of the contractor's staff shall be present at the TRRs and PTARs for facilitating institutional knowledge about incoming changes throughout the sustainment organization.

The contractor shall:

a. Perform installation and integration testing prior to formal IV&V testing.
b. Document all testing procedures including, but not limited to, test plans and scripts, data collection, checklists, schedule, and testing personnel.
c. Document contractor test findings in a Test Plan, Test Report, and Test/Use Cases (Section F, Deliverable 4.10).
d. Coordinate and provision test accounts for OT&E and user acceptance testing.
e. Identify and document defects and bugs in a Test Report and develop plans to address issues (Section F, Deliverable 4.10). Identify critical issues that would prevent the application from being released into the production environment.
f. Perform security compliance testing and address all known/unknown vulnerabilities.

C.5.4.1.4 TRANSITION AND DEPLOYMENT

Prior to deployment, all transition phase deliverables shall be reviewed and validated, software and/or hardware shall be tested, procedures shall be reviewed and validated, and knowledge transfer shall be complete between teams.

The contractor shall support the Production Readiness Review (PRR) as the final enterprise checkpoint or phase gate preceding production deployment (Section F, Deliverable 4.11). A checklist shall accompany the PRR as validation of the following:

1. Service Design/Development deliverables were completed and formally submitted to CM; project baseline artifacts, contractor Test Report, and OT&E test results with PTAR decisions.
2. Test Acceptance has been received from OT&E and Government Acceptance Testing (GAT) (if applicable); designated as a "Pass."
3. System accreditation was issued by the Designated Authority (DA).
4. The O&M staff is ready to deploy the product into production for sustainment.

Upon Government approval, the contractor shall lead and coordinate application deployment activities into production environments. The contractor shall coordinate with O&M transition teams and all relevant stakeholders to ensure the deployment is successful.

C.5.4.2 SUBTASK 4.2 – APPLICATION SUSTAINMENT

The contractor shall provide application sustainment support for all DCSA's planned and existing portfolio of applications. The contractor's sustainment efforts will ensure seamless transition, reliability, and availability for enterprise IT applications as well as the most cost-efficient strategy for O&M. Sustainment involves early engagement with the development teams and close coordination throughout the project lifecycle to ensure successful transition into the O&M environment. The contractor shall work with stakeholders (e.g., Government, third-party contractors) and provide subject matter expertise on behalf of the infrastructure and sustainment team. The contractor shall review and provide feedback on project plans, designs, scope, requirements, and deliverables to ensure compatibility and integration with the existing and future enterprise. Once transitioned, the contractor shall provide the necessary infrastructure support and regular maintenance (e.g., adaptive, preventive, and corrective) for applications. The contractor shall provide support to the Technology Roadmap , which is necessary for successful sustainment (Section F, Deliverable 4.16).

Sustainment support of this system will require personnel to be cleared at the Top Secret (TS)/Sensitive Compartmented Information (SCI) level.

C.5.4.2.1 PLANNING, REQUIREMENTS, AND DESIGN

The contractor shall participate in technical exchanges, working groups, and other meetings in the initial phases of a project. The contractor shall assess initial project plans, requirements, and designs to ensure compatibility, security, and integration with the current and future IT enterprise environment. The contractor shall propose recommendations and technical advice that improve the plans and designs as well as risk assessments. Prior to OT&E application testing phase, the contractor shall perform quality assurance checks of all custom code and conduct a Risk Assessment (Section F, Deliverable 4.12). The contractor shall ensure uniformity of coding standards from initial development through O&M. The contractor shall review final project plan deliverables.

The contractor shall:

a. Provide quality assurance and risk assessments prior to and during the initial phases of planning and development (Section F, Deliverable 4.12).
b. Provide weekly status reports on relevant information concerning each project (Section F, Deliverable 4.1).
c. Maintain a schedule for all sustainment projects, including pending actions, next steps, and milestones for all projects being supported.
d. Develop, maintain, and archive documentation pertaining to project phase.
e. Coordinate project scope, requirements, and schedules with application development and infrastructure support teams.
f. Proactively set up appropriate test environments.
g. Review and approve final technical design and specifications prior to development (Section F, Deliverable 4.14).
h. Identify potential licensing gaps.
i. Track baseline changes through CM Best Practices.
j. Conduct Quarterly Program Reviews on development activities (Section F, Deliverable 4.13).
k. Provide IA system validation and assessments.
l. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).

C.5.4.2.2 TESTING AND DEPLOYMENT

The contractor shall ensure test environments are maintained and replicate production environments. The contractor shall provide consulting and assessments during application testing phases. The contractor shall coordinate sustainment resources in advance of deployment to ensure project documentation and knowledge transfer is conducted. The contractor shall review and approve final project plans, requirements, and deliverables prior to deployment.

The contractor shall:

a. Proactively configure and maintain test environments.
b. Develop and maintain documentation pertaining to the project phase.
c. Conduct knowledge transfer.

d. Develop an Application Sustainment Plan identifying scope, resources, and costs (Section F, Deliverable 4.15).
e. Coordinate deployment of applications into the O&M environment.
f. Provide recommendations to improve application integration and performance prior to deployment.
g. Identify critical issues that would prevent the application from being released into the production environment.
h. Update the DCSA Run Book as needed (Section F, Deliverable 3.5).
i. Provide IA system validation and assessments.
j. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).

C.5.4.2.3 OPERATION AND MAINTENANCE (O&M)

The contractor shall provide O&M for enterprise applications. The contractor shall monitor application performance, troubleshoot issues, recommend solutions, and implement Government-approved changes. The contractor shall perform minor software maintenance (e.g., adaptive, preventive, corrective, bug fixes). Prior to conducting software maintenance that involves code updates/modifications/changes, the contractor shall perform a Quantitative Code Assessment that accurately determines the percentage of lines of code to be modified (Section F, Deliverable 4.18).

The contractor shall:

h. Monitor application and conduct incident management support.
i. Ensure application STIG compliancy.
j. Perform software maintenance (e.g., adaptive, preventive, corrective, bug fixes) in accordance with warranty and software licensing agreements.
k. Conduct application vulnerability management.
l. Perform hardware and software upgrades and patches.
m. Provide ad-hoc reporting, data management, and back-end data support for users.
n. Detect, troubleshoot, and resolve issues or outages that affect the performance of applications.
o. Work with approved subcontract vendors to ensure software maintenance is conducted in accordance with warranty and licensing agreements.
p. Recommend solutions and implement Government-approved changes to resolve issues.
q. Support Agency-wide Enterprise Architecture based on knowledge of existing and planned infrastructure.
r. Maintain active listing of software and hardware licenses.
s. Provide IA system validation and assessments.
t. Maintain DCSA accreditations and ensure current and accurate artifacts are uploaded to the DoD repository (eMASS).
u. Adhere to established application performance baselines in accordance with DCSA\DoD standards.
v. Perform lifecycle maintenance and application upgrades.

C.5.5 TASK 5 – ASSET MANAGEMENT

The contractor shall develop and implement a mature enterprise-wide IT Asset Management program. The contractor's program shall track, manage, and coordinate the purchase of new equipment (hardware/software), replacements, and upgrades. The contractor shall proactively plan and identify upgrades, updates, and end-of-life planning. The contractor shall process end-of-life, defective, and/or damaged equipment appropriately. In coordination with the tasks, the contractor shall develop an IT Life Cycle Management Plan (LCMP) for all equipment, hardware, and software within scope of the EITS Task Order (Section F, Deliverable 5.2). The contractor shall provide weekly, monthly, and ad-hoc reports as required (Section F, Deliverables 1.1, 5.1, and 5.5).

The contractor shall:

a. Provide a monthly report of all maintenance warranty and license agreements pertaining to DCSA IT hardware and software (Section F, Deliverable 5.3).
b. Provide early notification and coordination with DCSA TPOC and appropriate resource advisor of upcoming expirations of maintenance, warranty, or license agreements within 30, 60, 90, 120, 150, and 180 days.
c. Process end-of-life, defective, and/or damaged equipment through the Defense Reutilization Management Office (DRMO).
d. Monitor and maintain the equipment (hardware and software) license data repository that records and tracks all information pertinent to the lifecycle maintenance of the product (e.g., vendor name, software name and version, number of authorized users and/or devices covered, licensing fees, commencement, and expiration date).
e. Ensure equipment installed on DCSA networks is licensed and any software without an available license requires written permission from the DCSA TPOC.
f. Track and maintain an inventory of all equipment issued to DCSA personnel.
g. Deliver up-to-date equipment inventory lists and system data to the Government upon request (Section F, Deliverable 5.4).
h. Coordinate licensing, maintenance renewals, and warranty repairs with third-party vendors.
i. Maintain all non-user-based IT equipment inventory, including network printers and VTC components in conference rooms.
j. Provide support with shipping of equipment (e.g., using corrugated, packing material, and FedEx shipping forms).
k. Assist OCIO personnel with inventory support leveraging access to the Defense Property Accountability System (DPAS).

C.5 PERFORMANCE REQUIREMENTS SUMMARY

The Performance Requirements Summary (PRS) is provided in the below table.

Required Services (Tasks)	Performance Standards	Acceptable Quality Levels	Methods of Surveillance
Financial Reporting: Estimate to Complete (ETC) and Estimate at Completion (EAC); Cost incurred by task; percentage of funding expended; and estimated date(s) funding will be expended; Accumulated invoiced cost (Section C.5.1.2)	Reports accurately depict and track the current financial status of the contract.	100%	The FEDSIM COR with the assistance of the DCSA TPOC will monitor the monthly reports, invoices, and Technical Status Meetings (TSM) monthly
Status Reporting (minutes, briefings, presentation material) – (Sections C.5.1.2 and C.5.1.3)	Reports accurately depict current status	99%	The FEDSIM COR will inspect 100% of documents
Maintain all DCSA internet, NIPR, SIPR, and JWICS access points (Section C.5.3.1.1)	Networks are maintained to DoD standards	100%	The DCSA TPOC will review and inspect to ensure system performance
Update and maintain the SOPs to support database management (Sections C.5.3.4)	The Plan is timely and comprehensive and provides a high degree of confidence that the contractor's services and deliverables will be of a high quality	100%	The DCSA TPOC will review and inspect 100% of documents
Develop and implement a mature lifecycle process for conducting application development and sustainment of DCSA applications (Section C.5.4)	The Plan is timely, comprehensive, and provides a high degree of confidence that the contractor's services and deliverables will be of a high quality	100%	The DCSA TPOC will review and inspect 100% of documents

Required Services (Tasks)	Performance Standards	Acceptable Quality Levels	Methods of Surveillance
Deliver an Integrated Master Schedule detailing planned versus actual activities (project scope, schedule, costs, and product quality) (Section C.5.4.1.2)	The approved plan is followed precisely	100%	The DCSA TPOC with assistance from the FEDSIM COR will ensure the schedule is updated and followed
Perform hardware and software upgrades and patches (Section C.5.4.2.3)	Upgrades conducted timely	100%	The DCSA TPOC will perform periodic reviews to ensure compliance
Deliverable Compliance (Sections C.5.1 through C.5.5)	Deliverables comply with requirements outlined in the PWS and are submitted timely in accordance with Section F.3	99%	The FEDSIM COR with the assistance of the DCSA TPOC will perform periodic and random inspection of deliverables
Transition out Implementation (Section C.5.1.8)	The approved plan is followed precisely	100%	The FEDSIM COR with the assistance of the DCSA TPOC will perform periodic and random inspections and observations and review customer complaints
Final Quality Management Plan (Section C.5.1.10)	The Plan is timely and comprehensive and provides a high degree of confidence that the contractor's services and deliverables will be of a high quality	100%	The FEDSIM COR will inspect 100% of the documents

Required Services (Tasks)	Performance Standards	Acceptable Quality Levels	Methods of Surveillance
Contractor performing within expected resource usage. (Section C.5.1.6)	100% of resource usage is in line with the PMP	95%	The FEDSIM COR with the assistance of the DCSA TPOC will perform periodic and random inspections, observations and review of invoices, status reports, and customer complaints